

CLAIMS

1. A contents purveying system including a data processor having a reproduction program for reproducing contents data, a portable reproducing device for storing the contents data furnished from said data processor on a recording medium for reproduction and a contents server for distributing the contents data over a network to said data processor, wherein said data processor is configured so that

a first master key and a first authentication key are furnished to said reproduction program after installing said reproduction program, the contents data stored in an external storage medium connected to the data processor are acquired using said first master key for storage, said reproduction program executing authentication with respect to said portable reproducing device using the so-furnished first authentication key and first master key,

said data processor also being configured so that, when transmission/reception of the contents data distributed from said contents server to said reproduction program is made with said portable reproducing device, a second master key different from said first master key and a second authentication key different from the first authentication key are furnished over the network, the contents data furnished from said contents server are acquired using the so-furnished second master key for storage, and authentication with respect to the portable reproducing device is made using the so-furnished second authentication key and the second master key to effect transmission/reception of the contents data.

2. The contents purveying system according to claim 1 wherein said portable reproducing device holds first to i'th authentication keys updated in generation from the first to the i'th generation, i being an integer equal to 2 or larger, and first to i'th master keys updated in generation from the first to the i'th generation, i being an integer equal to 2 or larger;

said reproducing program being furnished over the network with second to i'th authentication keys updated in generation from the second to the i'th generation, i being an integer equal to 2 or larger, and second to i'th master keys updated in generation from the second to the i'th generation, i being an integer equal to 2 or larger;

said portable reproducing device performing reciprocal authentication with said reproduction program using the authentication key of the same generation.

3. The contents purveying system according to claim 2 wherein if said portable reproducing device performing reciprocal authentication with said reproduction program is using an authentication key and a master key of a generation older than the generation used by said reproduction program, the portable reproducing device updates the own authentication key and master key until the generation used by said reproduction program.

4. The contents purveying system according to claim 2 wherein if said reproduction program performing reciprocal authentication with said portable reproducing device is using an authentication key and a master key of a generation older than that used by

said portable reproducing device, said reproduction program asks said contents server for a key to update the own authentication key and the own master key up to the generation used by said portable reproducing device.

5. The contents purveying system according to claim 2 wherein, if accessed by said contents server, said contents server furnishes an authentication key and a master key of a generation later than that of the authentication key used by said reproduction program to update the generation of the authentication key used by said reproduction program.

6. A contents purveying method including a data processor having a reproduction program for reproducing contents data, a portable reproducing device for storing the contents data furnished from said data processor on a recording medium for reproduction and a contents server for distributing the contents data over a network to said data processor, wherein

a first master key and a first authentication key are furnished to said reproduction program after installing said reproduction program, the contents data stored in an external storage medium connected to the data processor are acquired using said first master key for storage, said reproduction program executing authentication with respect to said portable reproducing device using the so-furnished first authentication key and first master key, and wherein

when transmission/reception of the contents data distributed from said contents server to said reproduction program is made with said portable reproducing device, a

second master key different from said first master key and a second authentication key different from the first authentication key are furnished over the network, the contents data furnished from said contents server are acquired using the so-furnished second master key for storage, and authentication with respect to the portable reproducing device is made using the so-furnished second authentication key and the second master key to effect transmission/reception of the contents data.

7. The contents purveying method according to claim 6 wherein said portable reproducing device holds first to i 'th authentication keys updated in generation from the first to the i 'th generation, i being an integer equal to 2 or larger, and first to i 'th master keys updated in generation from the first to the i 'th generation, i being an integer equal to 2 or larger;

said reproducing program being furnished over the network with second to i 'th authentication keys updated in generation from the second to the i 'th generation, i being an integer equal to 2 or larger, and second to i 'th master keys updated in generation from the second to the i 'th generation, i being an integer equal to 2 or larger;

said portable reproducing device performing reciprocal authentication with said reproduction program using the authentication key of the same generation.

8. The contents purveying method according to claim 7 wherein if said portable reproducing device performing reciprocal authentication with said reproduction program is using an authentication key and a master key of a generation older than the

generation used by said reproduction program, the portable reproducing device updates the own authentication key and the own master key up to the generation used by said reproduction program.

9. The contents purveying method according to claim 7 wherein if said reproduction program performing reciprocal authentication with said portable reproducing device is using an authentication key and a master key of a generation older than that used by said portable reproducing device, said reproduction program asks said contents server for a key to update the own authentication key and the own master key up to the generation used by said portable reproducing device.

10. The contents purveying method according to claim 7 wherein, if accessed by said contents server, said contents server furnishes an authentication key and a master key of a generation later than that of the authentication key used by said reproduction program to update the generation of the authentication key used by said reproduction program.

11. (Added) A method for furnishing key data to a data processing apparatus, wherein
a first key is furnished to said data processing apparatus on which a contents reproducing program has been installed;

said first key data being used for acquiring contents data stored in an external recording medium for storage in said data processing apparatus, said first key data also being used in authentication for transmission/reception of said contents data with a portable reproducing apparatus connected to said data processing apparatus;

if said portable reproducing apparatus and the program reproducing program from said data processing apparatus effects transmission/reception of contents data distributed from said contents server,

second key data different from said first key data is furnished over a network; and wherein

said second key data is used for acquiring contents data furnished from said contents server for storage in said data processing apparatus, said second key data also being used for authentication of said data processing apparatus and said portable reproducing apparatus in order to effect transmission/reception of the contents data from said contents server.

12. (Added) The method for furnishing key data according to claim 11 wherein the ID information of said portable reproducing apparatus and key data of an i th generation are transmitted to said data processing apparatus and wherein the generation of key data of said portable reproducing apparatus is updated based on the ID information of said portable reproducing apparatus.

13. (Added) The method for furnishing key data according to claim 11 wherein the said portable reproducing apparatus holds the first to i th key data updated in generation from the first generation to the i th generation, where i is an integer not smaller than 2; and wherein

second to i th key data, updated in generation from the second to the i th generation, where i is an integer not smaller than 2, are furnished to said contents

reproducing program over a network; whereby

said portable reproducing apparatus and the contents reproducing program performs authentication using an authentication key of the same generation.

14. (Added) The method for furnishing key data according to claim 11 wherein, when accessing is made from said contents reproducing program, key data of a generation newer than the generation of the key data used by said contents reproducing program is furnished to said contents reproducing program to update the generation of the authentication key used by said contents reproducing program.

15. (Added) The method for furnishing key data according to claim 11 wherein said first key is a ripping key for ripping contents from a compact disc.

16. (Added) The method for furnishing key data according to claim 11 wherein said second key is a server connecting key for downloading contents from a contents server.

17. (Added) The method for furnishing key data according to claim 11 wherein said first key data includes a first master key and a first authentication key; and wherein said second key data includes a second master key and a second authentication key.

18. (Added) The method for furnishing key data according to claim 11 wherein said first key data is furnished from an external storage medium.

19. (Added) The method for furnishing key data according to claim 11 wherein said first key data is furnished from a server device.

20. (Added) The method for furnishing key data according to claim 11 wherein said second key data is furnished from a server device.

21. (Added) An apparatus for furnishing key data to a data processing apparatus, comprising:

transmission means for transmitting a first key to said data processing apparatus on which a contents reproducing program has been installed;

said first key data being used for acquiring contents data stored in an external recording medium for storage in said data processing apparatus, said first key data also being used in authentication for transmission/reception of said contents data with a portable reproducing apparatus connected to said data processing apparatus; wherein

if said portable reproducing apparatus and the program reproducing program from said data processing apparatus effect transmission/reception of contents data distributed from said contents server,

said transmission means furnishes second key data different from said first key data over a network; and wherein

said second key data is used for acquiring contents data furnished from said contents server for storage in said data processing apparatus, said second key data also being used for authentication of said data processing apparatus and said portable reproducing apparatus in order to effect transmission/reception of the contents data from said contents server.

22. (Added) A data processing apparatus including a contents reproducing program for

reproducing contents data, in which the data processing apparatus is connected to an external storage medium and to a portable reproducing apparatus, and in which the data processing apparatus acquires contents data from said external storage medium and furnishes contents data furnished from said external storage medium to said portable reproduction apparatus, wherein

first key data furnished by said contents reproducing program for use in storing contents data supplied from said external storage medium is used for authentication in acquiring contents data stored in said external storage medium for transmission/reception; and wherein

when the contents reproducing program effects transmission/reception of the contents data distributed from a contents server, second key data different from said first key data is furnished over a network, said second key data furnished being used for authentication in acquiring contents data furnished from said contents server.

23. (Added) The data processing apparatus according to claim 22 wherein said contents reproducing program is included in a comprehensive management unit processing the copyright management, said comprehensive management unit being stored by being installed from an external storage medium.

24. (Added) The data processing apparatus according to claim 23 wherein key data for the 0th generation as said first key data is acquired at the same time as said comprehensive management unit is installed.

25. (Added) The data processing apparatus according to claim 22 wherein said first

key data is furnished by an external storage medium.

26. (Added) The data processing apparatus according to claim 22 wherein said first key data is furnished from a server device.

27. (Added) The data processing apparatus according to claim 22 wherein said second key data is furnished from a server device.

28. (Added) The data processing apparatus according to claim 22 wherein the key data is updated in generation by receiving the ID information of a portable reproducing apparatus acquired from a key data furnishing server and key data of the i th generation, and wherein said key data is transferred to the portable reproducing apparatus based on the ID information of said portable reproducing apparatus to update key data of said portable reproducing apparatus.

29. (Added) The data processing apparatus according to claim 22 wherein if the generation of the key data of the $(i+k)$ th generation of said portable reproducing apparatus is larger than the generation of the key data of the i th generation stored in said data processing apparatus, request of key data of the new generation is issued over a network to a key data furnishing server; key data of the $(j+k)$ th generation distributed from said key data furnishing server being received to update the generation of the key data.

30. (Added) A data processing method including a contents reproducing program for reproducing contents data, in which the data processing method is connected to an external storage medium and to a portable reproducing apparatus, and is used in a data

processing apparatus adapted for acquiring contents data from said external storage medium and for furnishing contents data furnished from said external storage medium to said portable reproduction apparatus, wherein

first key data furnished by said contents reproducing program for use in storing contents data supplied from said external storage medium is used for authentication in acquiring contents data stored in said external storage medium for transmission/reception; and wherein

when the contents reproducing program effects transmission/reception of the contents data distributed from a contents server, second key data different from said first key data is furnished over a network, said second key data furnished being used for authentication in acquiring contents data furnished from said contents server.

31. (Added) The data processing method according to claim 30 wherein said contents reproducing program is included in a comprehensive management unit processing the copyright management, said comprehensive management unit being stored by being installed from an external storage medium.

32. (Added) The data processing method according to claim 31 wherein key data for the 0th generation as said first key data is acquired at the same time as said comprehensive management unit is installed.

33. (Added) The data processing method according to claim 30 wherein said first key data is furnished by an external storage medium.

34. (Added) The data processing method according to claim 30 wherein said first key

data is furnished from a server device.

35. (Added) The data processing method according to claim 30 wherein said second key data is furnished from a server device.

36. (Added) The data processing method according to claim 30 wherein the key data is updated in generation by receiving the ID information of a portable reproducing apparatus acquired from a key data furnishing server and key data of the i th generation, and wherein said key data is transferred to the portable reproducing apparatus based on the ID information of said portable reproducing apparatus to update key data of said portable reproducing apparatus.

37. (Added) The data processing method according to claim 30 wherein if the generation of the key data of the $(i+k)$ th generation of said portable reproducing apparatus is larger than the generation of the key data of the i th generation stored in said data processing apparatus, a request of key data of the new generation is issued over a network to the key data furnishing server; key data of the $(j+k)$ th generation distributed from said key data furnishing server being received to update the generation of the key data.

38. (Added) A recording medium having stored therein a program for reproducing contents data, in which the recording medium is connected to an external storage medium and to a portable reproducing apparatus, and in which the program is executed on a data processing apparatus adapted for acquiring contents data from said external storage medium and for furnishing contents data furnished from said external storage

medium to said portable reproduction apparatus, wherein

the recording medium has stored therein a program which permits said data processing apparatus to operate in such a manner that

first key data furnished by said contents reproducing program for use in storing contents data supplied from said external storage medium is used for authentication in acquiring contents data stored in said external storage medium to effect transmission/reception; and that

when the contents reproducing program effects transmission/reception of the contents data distributed from a contents server, second key data different from said first key data is furnished over a network, said second key data furnished being used for authentication in acquiring contents data furnished from said contents server.

39. (Added) A portable reproducing apparatus connected to a data processing apparatus having a contents reproducing program for reproducing contents data, in which contents data furnished from said data processing apparatus is stored in a recording medium for reproduction, wherein

inherent ID information and key data of plural generations are stored from the outset;

key data of the same generation as the first key data supplied to said contents reproducing program in said data processing apparatus and used for storing the contents data furnished from an external storage medium connected to said data processing apparatus is used to effect authentication with said data processing

apparatus in acquiring contents data stored in said external storage medium connected to said data processing apparatus;

and wherein

when said contents reproducing program effects transmission/reception of contents data distributed from the contents server, second key data different from said first key data is furnished to said data processing apparatus over a network;

the key data of the same generation as the second key data furnished being used to effect authentication in acquiring the contents data furnished from said contents server to receive said contents data from said data processing apparatus.

40. (Added) The portable reproducing apparatus according to claim 39 wherein authentication keys of plural generations and master keys of plural generations are stored from the outset.

41. (Added) The portable reproducing apparatus according to claim 39 wherein said first key data is a ripping key for ripping contents data from a compact disc and wherein the contents data can be acquired from said compact disc by said ripping key.

42. (Added) The portable reproducing apparatus according to claim 39 wherein said second key data is a server connecting key for downloading contents data from a server device and wherein the contents data can be acquired from said server device by said server connecting key.

43. (Added) The portable reproducing apparatus according to claim 39 wherein if, in authentication with said contents reproducing program, key data of a generation older

than the generation used in said contents reproducing program is used, own key data is updated in generation up to the generation used by said contents reproducing program.

44. (Added) The portable reproducing apparatus according to claim 39 wherein first to i th key data, updated in generation from the first to the i th generation, are held, and wherein

key data of the same generation among second to i th key data furnished over a network from said contents reproducing program and updated in generation from the second to the i th generation, where i is an integer not smaller than 2, is used to effect authentication with said contents reproducing program.

45. (Added) A data processing method for use in a portable reproducing apparatus connected to a data ro apparatus having a contents reproducing program for reproducing contents data, said portable reproducing apparatus storing the contents data furnished from said data processing apparatus for reproducing the stored contents data, wherein

inherent ID information stored in said portable reproducing apparatus from the outset and key data of plural generations are used;

key data of the same generation as the first key data supplied to said contents reproducing program in said data processing apparatus and used for storing the contents data furnished from an external storage medium connected to said data processing apparatus is used to effect authentication with said data processing

apparatus in acquiring contents data stored in said external storage medium connected to said data processing apparatus to receive contents data stored in said external storage medium;

and wherein

when said contents reproducing program effects transmission/reception of contents data distributed from the contents server, second key data different from said first key data is furnished to said data processing apparatus over a network;

the key data of the same generation as the second key data furnished being used to effect authentication in acquiring the contents data furnished from said contents server to receive said contents data from said data processing apparatus.

46.(Added) The portable reproducing apparatus according to claim 45 wherein said first key data is a ripping key for ripping contents data from a server device and wherein the contents data can be acquired from said server device by said ripping key.

47. (Added) The portable reproducing apparatus according to claim 45 wherein said second key data is a server connecting key for downloading contents data from a server device and wherein the contents data can be acquired from said server device by said server connecting key.

48. (Added) The portable reproducing apparatus according to claim 45 wherein if, in authentication with said contents reproducing program, key data of a generation older than the generation used in said contents reproducing program is used, key data of said portable reproducing apparatus is updated in generation up to the generation used by

said contents reproducing program.

49. (Added) The portable reproducing apparatus according to claim 45 wherein first to i th key data, updated in generation from the first to the i th generation, are held, and wherein

key data of the same generation among second to i th key data furnished over a network from said contents reproducing program and updated in generation from the second to the i th generation, where i is an integer not smaller than 2, is used to effect authentication with said contents reproducing program.

50. (Added) A recording medium connected to a data processing apparatus having a contents reproducing program for reproducing contents data, in which the recording medium has stored therein a program executed by a portable reproducing apparatus adapted for storing and reproducing contents data furnished by said data processing apparatus, wherein

inherent ID information stored in said portable reproducing apparatus from the outset and key data of plural generations are used; and wherein

the recording medium has stored therein a program for permitting said portable reproducing apparatus in such a manner that

key data of the same generation as the first key data supplied to said contents reproducing program in said data processing apparatus and used for storing the contents data furnished from an external storage medium connected to said data processing apparatus is used to effect authentication with said data processing

apparatus in acquiring contents data stored in said external storage medium connected to said data processing apparatus to receive contents data stored in said external storage medium;

and wherein

when said contents reproducing program effects transmission/reception of contents data distributed from the contents server, second key data different from said first key data is furnished to said data processing apparatus over a network;

the key data of the same generation as the second key data furnished being used to effect authentication in acquiring the contents data furnished from said contents server to receive said contents data from said data processing apparatus.